「政府情報システムのためのセキュリティ評価制度(ISMAP)における各種基準(案)に対する意見

2020年4月24日

BSA | ザ・ソフトウェア・アライアンス (以下、BSA)[1] は「政府情報システムのためのセキュリティ評価制度（ISMAP）における各種基準（案）」について経済産業省、総務省、内閣サイバーセキュリティセンター、情報通信技術（IT）総合戦略室に対して以下の通り意見を提出します。

総論

BSA 会員企業は、クラウドコンピューティングを含む最先端の技術、製品、サービス又関連サービスの提供を通して、世界の情報経済と市民の生活向上に寄与しています。クラウドコンピューティングは現在、また、今後も最も重要な技術となっていくでしょう。特に現在のような世界的危機下においては、緊急の需要に応え、リモートワークを可能とするための重要かつ信頼できる機能を維持し、世界中の政府を支えています。従って、関連する規制や政策は安全なクラウドサービスの発展を後押しすべきであります。又、BSA は、クラウドサービスを含む政府調達においては、サイバーセキュリティの優先が重要であることも理解しております。

この点において、我々は、日本政府が政府全体における安全なクラウドサービス導入を促進するために継続的に努力を続けていること、また、ISMAP の策定段階において、利害関係者との意見交換の機会を設けてくれたことに感謝しております。BSA はクラウドサービスの安全性評価に関する検討会からの 2019 年 4 月の「中間とりまとめ（案）」に対して [2]、又、12 月の「とりまとめ（案）」に対して [3]意見を出しており、ISMAP における各種基準（案）に我々の意見を考慮に入れて頂いたことに感謝しております。

サイバーセキュリティの解決策として最も効果的なのは、リスクを起点とし、柔軟で成果志向である政策です。ISMAP はまだ策定段階ではありますが、この前提は概ね満たされていると我々は見ています。そして、この取り組みにさらに貢献するため、以下の提案を述べさせて頂きます。

---

[1] BSAの活動には、Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workdayが加盟企業として参加しています。詳しくはウェブサイト（https://bsa.or.jp/）をご覧ください。

[2] https://bsa.or.jp/wp-content/uploads/20190416j.pdf
[3] https://bsa.or.jp/wp-content/uploads/20191225j.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

提言

[ISMAP 管理基準（案）]
第 2 章/2.2.言明書に記載すべき内容/2.2.5 監査の対象となる期間

[ISMAP 情報セキュリティ監査　ガイドライン（案）]
第 4 章/4.5 他の認証・監査制度等の証拠の利用

ISMAP 管理基準（案）の 2.2.5 では、クラウドサービスリストに登録されるクラウドサービスの全ての管理基準について、毎年、監査が必要であると記されています。ISMAP 情報セキュリティ監査ガイドラインにおいて、標準監査手続の実施に他の認証・監査制度や内部監査等において収集された証拠を再利用することを認める旨が記されているものの、関連する先行投資は技術革新的であるクラウドサービスプロバイダー（CSP）にとっては障壁となります。監査手続は高額であるだけでなく、監査要求を満たすために、セキュリティ人員から本来の責務を果たす時間を奪うことにもなります。その点からも、多くの国際認証の手続においては、2 年もしくは 3 年ごとの監査要件となっており、それによってセキュリティが損なわれることもありません。このことからも、監査手続を簡略化し、CSP 側の不要な負担を最小限におさえる方法を引き続き模索して頂きたく思います。

ISMAP においては、頻度を減らした監査スケジュールを設定されることを我々は推奨します。クラウドサービスの複雑性によっては、ISO-27000 のような監査手続は長期に亘る活動となり、大がかりなシステム変更においては短くなることもありますが、通常は 3 年の期間を設けています。毎年監査が実施されることになれば、CSP は連続して監査プロセスを実施しなくてはならず、常時、監査対応に追われることとなります。また、調達省庁側にとっても、年度ごとの監査により関連する契約更新の負荷が増すことになります。官公庁の一般競争入札参加資格の登録制度における有効期間が 3 年ごとであることからも、監査に係る全ての ISMAP 関係者の作業を減らす上でも、監査期間を 3 年ごとに変更し、一般競争入札の要件と合わせることを奨めます。

我々はまた、IaaS（Infrastructure-as-a-Service）、PaaS（Platform-as-a-Service）、SaaS（Software-as-a-Service）といった、異なるクラウドコンピューティングのモデルに管理基準を合わせていくことを奨めます。これらのモデルは、CSP とクラウドサービスカスタマ（CSC）間の関係性や、責任共有における分配等、様々な点で異なります。

前述したように、BSA は ISMAP が日本の限られたクラウド監査人材に過剰な負荷をかけることになるのではないかと懸念しております。クラウドサービスの IT 監査や認証には高度な専門的技能が必要であり、国際的にもこれを効果的に実施できる有能な人材は限られています。世界における同様の制度においては、これが課題となりました。特に運用開始から最初の 2 年間においては、新たな要件で多数のクラウドサービス初めて認証を受けることになります。世界的に監査人が限られているということは、有能な職員が高額になることを意味します。これは、ISMAP を実施する省庁と CSP の間で妥当な範囲の期待と金額を協議すること、また、同時に、最も重要なシステムを防御するためには、高い技能をもった人員を世界的に育成する必要があることを意味します。

ISMAP に係わる CSP、監査人、政府にとっての限られた人材をより有効に活用するためにも、これらを考慮した上で、不可欠な管理策をさらに識別し、狭めることを奨めます。

監査人と CSP にとっての手続を能率的にするために有効なのは、ISMAP 管理基準に関する追加ガイドラインもしくは Q&A を数カ月内に策定して頂くことです。これにより、運用開始前に CSP は管理基準要件を正確に理解することができ、初期の評価活動を効率化することがで

きます。また、ISMAP の策定手続と並行して、日本のクラウドサービスのための IT 監査と認証人材を訓練し、技能を磨く手法を日本政府が策定することを推奨します。

[ISMAP クラウドサービス登録規則]
8 章サービス登録の有効期間

上記と同様の懸念となりますが、8.1 では、登録者は登録の対象となった監査の対象期間の末日の翌日から 1 年 4 カ月後までに、更新の申請をしなければならない、と記してあります。上記で述べておりますように、ISMAP のクラウドサービス登録期間を 3 年とすることを求めます。

第 4 章　サービス登録に関する申請/4.2、第 5 章　申請の受理/5.4 (1)、第 6 章　審査/6.1 (4)

上記においては、申請者によるサービス登録申請、問い合わせへの回答、また審査時の発見事項に係る統制の改善に関する期間が設定されていますが、現在の１ヶ月か２ヶ月という期間は、申請者が要件を完了するために十分な準備期間となっておりません。従って、期間は３ヶ月とすることを奨めます。

[ISMAP 管理基準（案）]
第 4 章　マネジメント基準/4.2. 記載内容について

4.2 では、CSC と CSP 間において、クラウドサービスにおける情報セキュリティリスクについて情報交換することが非常に重要である、と記しています。CSP とリスクに関して情報交換することは、サイバーセキュリティの成果をあげるためには不可欠である、ということに我々は同意します。これに適合する国際規格は ISO27005:2018 となります。

また、日本政府が民間と公共部門から集めた政府ネットワークへの情報セキュリティリスクに関するあらゆる情報や機密情報を CSP とやりとりするために、日本政府が正式な仕組みを策定することを奨めます。政府のデータやサービスの保護のために適用すべき管理基準を CSP が適切に判断するためには、これが不可欠となります。

第 6 章　情報セキュリティのための組織
6.3.P クラウドサービス利用者及びクラウドサービス事業者の関係

ISMAP においては、政府のクラウドサービス調達において、適切なセキュリティ・レベルを確保するために一律的なアプローチをとっておりますが、政府期間のサービスは多様で、サービスの管理策は個別のクラウドサービス契約（クラウド SLA）で網羅されていることを ISMAP 関係者が理解することも重要です。ISMAP においては中核となる、基本的な管理策をまとめており、その他の管理策については、CSP と調達省庁間で、両者の共同責任の詳細も含め、ISMAP 制度での調達時に、クラウド SLA において合意されるという理解でおります。この点について ISMAP 関係者に対して明確化することを奨めます。

[ISMAP クラウドサービス登録規則]
第 9 章　情報セキュリティインシデント発生時の報告

9.1 においては、登録されているサービスについて情報セキュリティインシデントが生じた場合に CSP が報告することが記載されています。どのようなセキュリティインシデントが ISMAP 運営委員会に報告されるべきかが明確になっていると、報告実施において大変有効です。政府のサービスやデータがリスクに晒されるような大規模のセキュリティインシデントの際の連絡手段として、この規則が重要となってくることは理解しておりますが、報告における敷居が低すぎると、政府に影響を及ばさない、解決済みの、さして深刻でないセキュリティ事

象に ISMAP 運営委員会が忙殺されることとなります。従って、未解決、又、緊急で、データ損失や重大な影響を及ぼす結果となったセキュリティインシデントのみを報告とすることを奨めます。また、個人情報に関連するインシデントに関しては、個人情報保護法における漏えい報告要件と合致させることを求めます。

最後に、本案には報告に使う様式が添付されていないため、報告においてどのような情報が求められるのかを本登録規則において明確化して頂きたく考えます。

第 15 章　登録に係る異議申立て

ISMAP クラウドサービス登録規則の 15 章においては、申請者が指定の様式によってサービス登録に関する処置への異議申し立てを ISMAP 運営委員会あてにすることができるとしています。そのような意義申し立てには ISMAP 運営委員会による特定のクラウドサービスの登録拒否も含まれるかもしれませんが、本規則案には指定の様式が含まれていないため、どのような情報が提供されるべきかが明確でありません。決断に関する申し立ての際に求められる情報について、本規則に明確な記載をすることを求めます。

別表１．申請書の提出方法、様式 1-14

別表 1 には申請書は郵送とすることが記載されておりますが、日本政府がデジタルファーストを原則としていることからも、オンラインでの申請書提出を推奨します。

また、様式 1 から 14 が本案に添付されていないため、登録に際して求められる項目や情報を確認する上においても、実際の様式が ISMAP 関係者に公開されると助かります。

[政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程（案）]
第 9 章　その他

9.1 では ISMAP 運営委員会及び制度運営に携わる者は、秘密情報が無権限の者に伝わり、情報の機密性が損なわれることがないようにしなければならない、としています。しかし、この秘密保持がどのように実施されるのか、また、ISMAP の実施プロセスの中で、別途詳細な秘密保持契約（NDA）によって担保されるのかが、明確ではありません。ISMAP 関係者が意見できるように、この点に関して提示頂けると助かります。

第 1 章　総則/1.4.5　ISMAP 運営委員会

今後の手続きに透明性をもたらすためにも、ISMAP 運営委員会の構成員、又、議事録の公開も含め ISMAP 運営委員会における協議内容が ISMAP の利害関係者とどのように共有されるのかも明確にして頂けるようお願い致します。

[結び]

本意見が ISMAP の各種基準を完成させる上で参考となることを願うとともに、公共分野において、安全で効率的なクラウドコンピューティング・ソリューションをさらに広く普及させるために協力していきたく存じます。本意見に関するご質問、また、意見交換に関し、いつでもご連絡ください。